UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/588,828	06/07/2000	Eric J. Sprunk	18926-002010US	9516

7590 07/02/2004

Philip H Albert
Townsend and Townsend and Crew LLP
8th Floor
Two Embarcadero Center
San Francisco, CA 94111-3834

EXAMINER	
SEAL, JAMES	
ART UNIT	**PAPER NUMBER**
2135	7

DATE MAILED: 07/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/588,828	SPRUNK ET AL.	
	Examiner	Art Unit	
	James Seal	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 5.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Action is in response to applicant's correspondence of 22 March 2004.

2. New claims 2-5 have been entered.

3. Claims 1-5 are pending

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

5. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Yorke-Smith US 5548648 A.

6. As per claim 1, the limitation of encrypting information (data) by plurality of encryption keys to be sent over a communication system (e.g. message) is taught by Yorke-Smith in Column 1, lines 6-8 . The limitation that the information is split into blocks (data segments) of predetermined lengths is disclosed by Yorke-Smith, Column 3, lines 25-29. Note the number L_2 is generated for each segment and that determines the length of data segment, hence the length of each block is predetermined. The limitation first key K_1 is used to encrypt a data segment DS_1 and a second key K_2 used to encrypt a data segment DS_2 is taught Column 4, lines 1-2 where j = 2 . Note Figure 3 shows the break up of the data information into data segments DS_1 , DS_2, ... DS_n . Each segment being encrypted under a different key to obtain encrypted data segments EDS_1, EDS_2, ... EDS_n The limitation that the second portion of the message overlaps the first portion of the message (see figure 3). Note that the fields of encrypted data include random numbers X which fills in between the other fields in the blocks not

including the control block or the encrypted data block (Column 4, lines 54-56). Note further that the position of the encrypted data block varies dependent on the random number S. As the random numbers X that pads the encrypted data blocks (which meets the limitation of the added one or more bits of information) vary also with S and the length of the encrypted data block its L_1 of themselves constitute part of the encrypted data (Column 3, lines 43, 44, 45-46), the the boundary between the encrypted data blocks will change relatively to the sequence of transmitted information and will thus constitutes an overlap region between the two encryption fields. Claim 1 is rejected.

Claim 2 rejected under 35 U.S.C. 103(a) as being unpatentable over **Yorke-Smith as applied to claim 1 above, and further in view of Koopman US 5619575.

7. As per claim 2, Yorke-Smith is silent on the limitation of adding (via concatenation) a authentication block in order to authenticate the encrypted message. Koopman teaches the appending to the encrypted message an authentication block Column 2, lines 29-49. It would have been obvious for one of ordinary skill in the art at the time the invention was make to have modified the invention of Yorke-Smith with that of Koopman because authentication of the message sent over a communication length provides proof that the message is indeed authentic. Further concatenating it to the message would have been obvious to one of ordinary skill in the art at the time the invention was made to have used concatenation as a means of including the message as Koopman uses concatenation because Koopman's encryption requires the use concatenation and thus to for the authentication block wouldn't require new equipment.

The limitation of encrypting the authentication block Koopman is silent, it would have been obvious for one of ordinary skill in the art to encrypt the authentication block to prevent replay attacks, which would occur if the information were sent in the clear. Although Koopman is silent on whether the authentication block is a predetermined length, most authentication use a hash function which generates a fixed length block, for example SHA-1 is 160 bits. Subdividing the concatenation field into predetermined block lengths is disclosed by Yorke-Smith (e.g., see abstract). As Yorke-Smith can subdivide the data blocks into equal or unequal lengths and into as many subdivisions and then designate one of the resulting cipher blocks as a designated cipher block, and the other cipher block as being non-designated cipher blocks is a matter of choice and certainly the combined lengths of the subdivisions would equal to the total block length. Note that the residue, in the case that the block is broken up into equal blocks can also accommodated by the Yorke-Smith device. The limitation of encrypting the first portion with one key and the second portion and residual portion together with the authentication block using a second key would have been obvious to one of ordinary skill in the art because the two pieces encrypted under different keys could be used to authenticate. The limitation of providing at least the first portion of the designated cipher block, the nondesignated cipher block and the cipher residual block as the message and this message could be decrypted if the authentication is disclosed by Koopman (see Column 2, lines 46-49). Claim 2, is rejected.

8. As per claim 3, the limitation that the subdivision of the message involves non-empty sets of bits would have been obvious to one of ordinary skill in the art in order to implement claim 2. Claim 3, is rejected.

9. As per claim 4, the limitation that the second authentication block comprises one or more bits forming a null value (all bits zero bits). It would have been obvious to one of ordinary skill in the art at the time that the invention was made, to have used a null value as the simplest means of validating a message. Claim 4 is rejected.

10. Claim 5, recites a encryption and corresponding decryption system with message authentication corresponding to the encryption with message authentication claimed in 2. Claim 5 is rejected.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JWS

Jws
AU 2135
29 May 2004

KIM VU
SUPERVISORY PATENT EXA...
TECHNOLOGY CENTER 21...